(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 December 2000 (14.12.2000)

PCT

(10) International Publication Number
WO 00/75749 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number: PCT/US00/15827

(22) International Filing Date: 8 June 2000 (08.06.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/328,422 9 June 1999 (09.06.1999) US

(71) Applicant *(for all designated States except US)*: **INTELISHIELD.COM, INC.** [US/US]; 10200 W. 44th Avenue, Suite 339, Wheat Ridge, CO 80033 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **FLOYD, Dennis, R.** [US/US]; 3265 Fenton Street, Denver, CO 80212 (US). **HEATON, Timothy, L.** [US/US]; 10875 W. 77th Drive, Arvada, CO 80005 (US). **ANDERSON, Brian, S.** [US/US]; 8755 W. 80th Avenue, Arvada, CO 80005 (US). **ANDERSON, Stanley, W.** [US/US]; 8755 W. 80th Avenue, Arvada, CO 80005 (US).

(74) Agent: **FOLEY & LARDNER**; 777 East Wisconsin Avenue, 33rd Floor, Milwaukee, WI 53202-5367 (US).

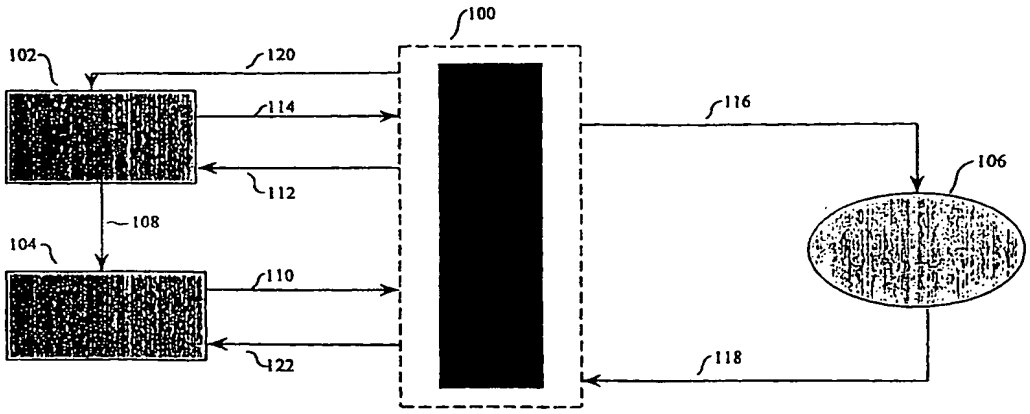
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *Without international search report and to be republished upon receipt of that report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: INTERNET PAYMENT SYSTEM



(57) Abstract: The present invention is a system and method for providing electronic commerce without providing a consumer's credit card data over the Internet, or any other public network. Consumers have a fear of providing their credit card data over the Internet. The present invention allows a consumer to make a purchase with their credit card without providing their credit card data over the Internet. The present invention provides consumers with a surrogate card number to make Internet purchases and the consumer personally authorizes their purchases while they are on-line. The consumer's actual credit card data is never transmitted over the Internet. The on-line affirmation of each purchase through the third party entity that provides the service described by this invention leads to a reduction of fraud.

WO 00/75749 A2

Internet Payment System

FIELD OF THE INVENTION

The present invention relates to Internet commerce, also known as electronic commerce. More particularly to credit card purchases over the Internet.

RELATED APPLICATION

This application claims the benefit of U.S. Provisional Application serial number 60/130,121, filed April 20, 1999 and entitled "Internet shopping without transferring credit card data over the Internet".

BACKGROUND OF THE INVENTION

The Internet, world wide web (WWW) is growing rapidly. Electronic commerce has grown substantially year after year. However, consumers still remain wary of making purchases over the Internet for fear of credit card fraud.

Since the Internet is a public network, consumers are fearful of providing their credit card data. Many electronic commerce options are available. None have been able to strike a balance between a system and process that is safe for the consumer, easy for the consumer, alleviates consumer fear, and does not disrupt the current system that merchants currently use.

When a consumer chooses to make a website on-line purchase they may use a credit card. Websites will require the consumer's name, credit card data, expiration date and typically the consumer's address, as well as the address the consumer would like the purchased items shipped to. When providing this data, a consumer types it into their browser, which transmits the data over the Internet, which is a public network. This transmission is not secure, and may be intercepted.

The consumer does not know how secure the server receiving their data is. Even if the transmitted data is not intercepted, someone may still be able to steal the data out of the website's server.

Websites allow consumers to save their credit card data: actual credit card number, expiration date, name on the card, and other personal information, in the website's database. The next time the consumer shops, their data will be available without the need to type in the data. Once a consumer purchases items at multiple websites, the consumer's credit card data is held by multiple databases on the Internet. Having data in more than one place increases the odds of having data stolen or intercepted.

Secure web-browsers exist, which encrypts the information being sent from the consumers browser to the website server. Typically secure web-browsers use Secure Socket Layer (SSL) technology. Secure servers also exist which utilize encryption, firewalls, and other means in an attempt to save consumers data from being stolen.

However, even with these secure measures the consumers credit card data is still being sent over the Internet. Servers housing the credit card data, often after it has been decrypted, are accessible, connected to the Internet and, and can be breached by hackers.

An example of current systems and processes is shown in Figure 2, a block diagram illustrating the current e-commerce process and typical credit card transaction process. Figure 2 illustrates a typical credit card transaction process with either a non-Internet merchant 200 or an Internet merchant 202, in which the process is the same.

Consumer 204 decides to make a purchase with either merchant (a non-Internet merchant 200 or an Internet merchant 202) . Consumer 204 then provides their credit card data to either merchant, represented by lines 208. Either merchant sends the credit card data to standard credit card approval network 206, line 210.

Standard credit card approval network 206 then processes the order and signifies to either merchant whether the transaction has been approved or disapproved, line 212. Either merchant then informs consumer 204 whether the transaction has been approved or disapproved, line 214.

Current systems allow either merchant to view consumer's 204 credit card data. The Internet merchant, through interaction with consumer 204, also receives the data, line 208, over a public network, the Internet.

Other options exist, two patents are discussed below.

U.S. Patent No. 5,826,241 ('241) discloses a computerized system for making payments and authenticating transactions over the Internet. The '241 patent requires both the consumer and the merchant to have an account with the system. The '241 invention inserts itself into each financial transaction, charges the consumer's credit card, receives payment from the company the consumer has a credit card merchant account with, may remove credit card fees and service charges, and then passes the money onto the merchant. The merchant is paid long after the purchase is consummated, maybe 30 days or more. Electronic mail (E-mail) is used to verify a purchase with a consumer, which may be a time consuming process. Transactions are approved by the consumer via email utilizing either "yes", "no", or "fraud" in the E-mail messages. The '214 patent uses the consumers' surrogate credit card number as the personal identification number (PIN) and shares the surrogate credit card number with the merchant.

U.S. Patent No. 5,757,917 ('917) discloses a computerized payment system for purchasing goods and services on the Internet. Transactions are approved by the consumer via E-mail utilizing either "yes", "no" or "fraud" messages, which are slow and time-consuming. The '917 patent uses the consumers' surrogate credit card number as the personal identification number (PIN) and shares the surrogate credit card number with the merchant. The '917 patent also uses hardwired ethernet connections between a an Internet-connected computer, "front end" and a computer, "back end", which contains both the surrogate and actual credit card data and which communicates with the credit card approval network.

Consumers are wary of how their data is transmitted, who has access to the data, where the data is being stored, how long the data is being stored, and how secure the server storing the data is.

A need exists for storing consumers' credit card data securely and keeping the data from ever being transmitted over a public network such as the Internet.

There is a need to facilitate electronic commerce credit card transactions in a secure and time-efficient manner without changing the current credit card merchant account systems that presently exist. A standard credit card processing method exists and is currently used by every merchant who accepts credit cards. A system that requires merchants to acquire new accounts or to otherwise alter their standard order processing system may not be cost effective or may be unacceptable to merchants.

Merchants may not want to sign up for another service, apply for the service, go through the typical credit and background checks, which result in the need to set up additional accounting procedures, and receive yet another monthly statement and invoice. Merchants need a system that alleviates consumer fears and requires no additional hardware, software, or other costly and time consuming procedures to implement.

A need exists for consumers, who decide to make a purchase to securely make purchases over the Internet with as little effort and disruption as possible for either the consumer or the merchant, without abandoning the present credit card processing method.

Until the present invention, the foregoing needs and problems had not been met or solved.

FEATURES AND ADVANTAGES

The present invention has multiple features and advantages, a few of which are discussed below, others will be apparent from the entire disclosure.

The present invention eliminates consumer fears about releasing credit card data. Consumers' credit card data is kept securely and never transmitted over a public network such as the Internet.

With the present invention it is not necessary for merchants to sign up for another service, purchase additional hardware, nor software. The code that controls the merchants' Internet order forms is simply modified by the provider of the service described in this

invention. The entire process may be transparent to the merchant, or the merchant may participate if so desired.

When using the present invention, as far as the merchant is concerned, the standard credit card transaction takes place and the merchant receives their payment through their merchant account provider just as with any other of their credit card transactions.

A merchant does not need a secure site, digital identification certificate, and other time consuming and expensive additions to their website for the purpose of providing secure transmissions for Internet commerce when using the present invention. Credit card data is never sent over a public network, such as the Internet.

The present invention maintains a point of sale (POS) terminal for each member merchant. The POS is connected over secure telephone lines to the merchant's processor, the same as any of the merchant's other POS terminals. Therefore, the approval process takes only seconds.

Due to the present invention, wherein a third party confirms each on-line purchase, merchants may be the victims of less fraud.

Only the consumer needs an account with the provider of the service described herein. The merchant does not need such an account. Consumers receive accounts by subscribing to the service described herein. A consumer receives a surrogate credit card number and personal identification number (PIN). Neither the credit card data, nor the surrogate credit card number, nor the PIN is ever revealed to the merchant. The consumer's credit card data is kept on a secure server which is never transmitted over the Internet.

Consumers personally enter their credit card data into the secure server using a PBX (Public Exchange) line just as they presently do when activating a new credit card with their card issuer. Consumers may enter credit card data for multiple cards which may allow the consumer the flexibility of choosing which card to make a purchase with.

Accordingly, the credit card data is not accessible to the employees who operate the present invention, which is a further security enhancement of the present invention.

The consumer invokes the present invention by clicking an icon on the merchant's standard Internet order form. The invocation of the present invention is done instantly and in real-time.

The consumers' credit card data is kept on a server located behind a firewall, and multiple other security barriers, which are not connected to the Internet. The server containing the credit card data uses multiple layers of security that permanently isolate the server from both the consumer and merchant transactions and the credit card approval loop. The server containing the credit card data is never directly connected to any data transmission capability.

Working in conjunction with enhanced networking security protocols, the server also utilizes advanced multi-layered data mining and data management application programming interfaces to protect the internal data structures from data access outside of the standard transaction process. Additionally, the server utilizes multiple data filters to prevent data outflows from transmission pathways other then those included in the transaction process. These processes, along with multiple gateways and firewalls, effectively isolate the server from the Internet, the internal Intranet, the telecommunication network used by the PBX system, and the external credit card authorization network.

Special software does not need to be loaded onto the consumer's computer. The consumer may use any computer, anywhere, without the need for installing special software.

The present invention also checks the consumers preferred shipping address with the address provided by the consumer at the time of purchase. This check provides yet another level of security. If a credit card is lost, a criminal could order merchandise and have it shipped to the criminals account. If the surrogate credit card number is lost, the criminal must also know the PIN number to be able to purchase merchandise with the account. Even if the PIN number is lost, the merchandise will only be shipped to the address

contained on the secure server. The criminal will not be able to send the merchandise to an address of the criminal's choosing without entering another verification number which is other than the surrogate credit card number or the PIN number, such as a portion of the person's social security number or the name of a relative, i.e. data that would not be known to the criminal.

Another level of consumer security comes from the fact that the consumer's credit data is only on one server, not spread through out the internet on multiple merchant servers. Therefore, the consumer may inactivate their account by only having to access only one server, which denies use of the consumer's credit card data by everyone.

A consumer is able to validate their purchase in real time while on-line. A transaction only occurs after correct verification of the surrogate credit card number, PIN, and shipping address.

SUMMARY OF THE INVENTION

The present invention is a system and method for providing electronic commerce without providing a consumer's credit card data over the Internet, or any other public network. The consumer uses a surrogate credit card number to make purchases over the Internet. An ultra-secure server network is provided in which the surrogate credit card number can only be translated into the actual credit card data when the consumer, who is on-line while a purchase is being made, personally authorizes the purchase using a separate personal identification number. The converted credit card data is transmitted directly to the bank that handles the merchant's credit card account, just as though the consumer's actual credit card were physically passed through a point-of-sale terminal at the merchant's premises. The data then proceeds through the standard electronic credit card approval loop. The surrogate card issuer acts as a front-end, independent third party enabling prior consumer approval of each transaction while operating seamlessly with the standard credit card approval system.

BRIEF DESCRIPTIONS OF THE DRAWINGS

A more complete appreciation of the invention and many of the attendant advantages thereof will become better understood when referring to the accompanying drawings wherein:

Figure 1 is a block diagram illustrating the process of the present invention.

Figure 2 is a block diagram illustrating the current e-commerce process and standard credit card transaction process.

Figure 3 is a block diagram illustrating the process of the present invention as shown in Figure 1, in more detail.

Figure 4 is a block diagram illustrating the overall process of the present invention between servers.

Figure 6 is a block diagram of the transaction process for the present invention.

Figure 7 is a block diagram continuing the transaction process of Figure 6 for the present invention.

Figure 8 is a block diagram illustrating a step from Figure 7 with additional steps.

Figure 9 is a block diagram of the process for establishing a consumer's account with the present invention.

Figure 10 is a block diagram of the process for establishing a merchant's membership with the service that implements the present invention.

DETAILED DESCRIPTION OF THE INVENTION

Referring now to the figures, figure 1 is a block diagram illustrating the process of the present invention. The present invention internal network 100 is illustrated by block

100. Consumer 102 interacts with merchant 104. Transactions are made through a standard credit card approval network 106.

Lines labeled 108 through 122 illustrate the process of the present invention. Line 108 illustrates consumer 102 choosing to purchase a product or service and utilize internal network 100. Merchant 104 sends the following to internal network 100: merchant ID, transaction amount, indicated shipping address (as typed in by the member), and merchant's 104 internal order number, line 110. Merchant 104 also sends the internet protocol address of consumer 102, line 110. Internal network 100 sends a Purchase Authorization Screen (PAS) to consumer 102, represented by line 112, by utilizing the internet protocol address supplied by merchant 104.

The PAS is displayed upon the consumer's 102 computer screen as a window which details to consumer 102 merchant's 104 name and transaction amount. The PAS then prompts consumer 102 to enter their surrogate credit care number and PIN to authorize the transaction. Consumer 102 sends this data to internal network 100, line 114.

Internal network 100 securely converts consumers surrogate credit card number to the actual credit card data necessary to conduct a credit card transaction. Line 116 transmits consumer's 102 credit card data to merchant's 104 merchant processor using a standard POS terminal for a standard credit card approval network 106. Consumer's 102 data is not sent over the Internet or any other public network.

Standard credit card approval network 106 then replies with either an approval or disapproval, 118. If approved, an order confirmation is sent to consumer 102 through line 120 and a confirmation is also sent to merchant 104 through line 122. Merchant 104 never views the consumer's surrogate credit card number, PIN number, nor credit card data.

The transaction is now complete, consumer 102 has made a purchase, merchant 104 has made a sale, and standard credit card approval network 106 has processed the credit card transaction. Neither merchant 104 nor standard credit card approval network 106 have seen or done anything different than they have done in the past.

Figure 3 is a block diagram illustrating the process of the present invention as shown in Figure 1, in more detail.

Blocks and lines, 100 through 122 are identical to Figure 1. Please read Figure 1 in conjunction with Figure 3. The following information describes the present invention internal network 100 in greater detail.

Internal network 100 consists of web server 300 which is connected to the Internet. Web server 300 registers consumers and receives transaction data from merchant 104, including: merchant ID, transaction amount, indicated shipping address (as typed in by the member), and merchant's 104 internal order number, line 110. Consumer 102 chooses to make a purchase of goods and/or services from merchant 104, line 108. Web server 300 then sends a PAS to consumer 102, represented by line 112.

The PAS then prompts consumer 102 to enter their surrogate credit card number and PIN. Consumer 102 enters the data, which is then passed back to web server 300. Web server 300 transmits, arrow 306, the data to server 303.

Server 303 is isolated from the Internet and is part of an intranet operated behind a secure firewall by the entity that provides the service described in this invention. Server 304 resides behind a gateway that incorporates multiple security barriers. Server 304 is only connected to an isolated, internal network connection and is permanently isolated from the Internet, consumer 102, merchant 104, and standard credit card approval network 106.

Server 303 then compares the surrogate credit card number and PIN for validation, line 314, and transmits a command through the secure gateway to server 304 which then converts the surrogate credit card number to the corresponding actual credit card data. The data from merchant 104 and consumer 102 actual credit card data is passed to terminal server 302, line 312. Terminal server 302 transmits the received data to the standard credit card approval network 106 through a POS terminal, which is maintained within terminal server 302, through a secure gateway, and over secure dedicated telephone lines, line 116. A POS terminal is maintained for each individual merchant 104, the standard credit card

approval network 106 does not know whether the credit card was processed by the present invention or merchant 104 directly.

The transmission from terminal server 302 to standard credit card approval network 106 is not over a public network, nor over the Internet, it is over secure telephone lines linking terminal server 302 to the standard credit card approval network 106.

Standard credit card approval network 106 then replies with either an approval or disapproval, line 118. The approval or disapproval is sent with an order confirmation number and actual credit card data over the same secure telephone lines to the merchant's POS terminal located within terminal server 302.

Terminal server 302 then transmits the order confirmation number, approval or disapproval, and actual credit card data to server 304, arrow 310. Server 304 then converts the credit card data back to consumer's 102 surrogate credit card number. Server 304 then transmits the order confirmation number and surrogate credit card number through the secure gateway to server 303, line 316. Server 303 then transmits the data through the firewall to web server 300, arrow 308.

Web server 300 then sends order confirmation, approval or disapproval, to consumer 102, line 120, and order confirmation, approval or disapproval, to merchant 104, line 122.

The transaction is now complete, consumer 102 has made a purchase, merchant 104 has made a sale, and standard credit card approval network 106 has processed the credit card transaction. Neither merchant 104 nor standard credit card approval network 106 have seen or done anything different than they have done in the past.

Figure 4 is a block diagram illustrating the overall process of the present invention between servers. Shown in Figure 4 are the pathways between the various servers, layers of security represented by the firewall, and the gateways. Consumer 102 and merchant 104 are connected to Internet 402. Web server 300 is connected to Internet 402 and to server

303 through security firewall 406. Server 303 is then connected to intranet 408 through gateway 410.

PBX System 404 is accessed by consumer 102 through conventional phone lines, line 401, to a specific phone at the number listed in consumers 102 subscription. Using PBX system 404 consumer 102 enters their actual credit card data through secure gateway 402 into server 304. Server 304 communicates with terminal server 302 through connection 412. Server 304 and server 302 are located in close proximity within a vault that has highly restricted access.

Terminal server 302 is connected to standard credit card approval network 106 through gateway 414, completing the system.

Figure 6 is a block diagram of the transaction process for the present invention. In step 600 the consumer decides to make a purchase at a merchant's website. In step 602 the consumer proceeds to checkout, to pay for the products or services selected.

In step 604, after successful completion of all data fields required by the merchant's Internet order system, including the shipping address, the consumer, when presented with the payment data options, selects to use the present invention as their payment vehicle and then submits their order. Selecting the present invention is as simple as clicking on an icon or text link which signifies the present invention and is recognized by the consumer.

In step 606 the merchant assigns an internal order number, having previously validated the data entered on the order entry screen. For example the consumer will enter a shipping address and the data entered needs to be verified, e.g. the zip code must be of a predefined length, etc.. This validation is done within the merchant's own network. If the data is not validated the member is passed back to the order entry screen to complete any required fields.

In step 608, upon validation of the data by the merchant, the transaction is passed to the present invention's web server. The data passed to the web server includes the following data: merchant ID, transaction amount, indicated shipping address (as typed in by the member), and the merchant's internal order number. Also passed to web server is

the Internet protocol (IP) address of the consumer who, at this point, is unknown by the entity that provides the service described in the present invention.

Figure 7 is a block diagram continuing the transaction process for the present invention. Step 610 prompts the consumer for verification of their order. Utilizing the consumers IP address as passed to the web server by the present invention's code that was inserted into the merchants web page; a PAS is sent to the consumer. The PAS is sent by the present invention's web server and not by the merchant. The following process steps are transparent to the merchant and the merchant does not know what is being done between the present invention's web server and the consumer.

The PAS is displayed upon the consumer's computer screen as a window that details to the consumer the merchant name and transaction amount. The PAS then prompts the consumer to enter their surrogate credit card number and PIN.

In step 612 web server queries the secure intranet server operated by the entity that provides the service described in this invention for validation of the consumer account ID, surrogate credit card account number, and PIN. Step 614 determines if the data is valid. If not valid then the consumer is prompted to re-enter the data again in Step 616, otherwise the process passes to step 618. If the data fails validation again, the member is prompted to contact consumer service and the web server sends the merchant a transaction fail notice.

Step 618 attempts another layer of security by querying the web server for verification of the address entered by the consumer on the merchant's system against the address contained within the web server. If the addresses match, the transaction continues to step 624. If the addresses do not match, because the consumer is shipping goods to another address, the consumer is asked to provide another validation in step 620. In step 620 the last four digits of the consumers social security number, or some other data that is not likely to be known to anyone other than the member-consumer, is requested to authorize the transaction. In step 622, if this supplemental data is valid, the transaction passes to step 624. Otherwise, if it is not valid, the transaction is declined and the

consumer is prompted to contact consumer service and the web server sends the merchant a transaction failure notice in step 628.

Step 624 sends the data to the merchant's processor via the standard credit card approval network, additional steps shown in more detail in Figure 8. Step 626 determines whether the merchant processor verified the transaction and completed the transaction. If the transaction was not completed, then a failure notice is sent to the merchant in step 628 and the process ends.

If the transaction was completed, a completion notice is sent to the merchant in step 630 containing the merchant's internal order number, and an approval notice provided by the merchant processor. The merchant receives the data into their e-commerce platform and continues to process the transaction in order for the goods to be shipped and the transaction closed.

Figure 8 is a block diagram that illustrates step 624 from Figure 7 with additional steps. Step 800 begins the process in which the web server converts the member ID and PIN into an internal routing number. In step 802 the web server then passes the following data to the gateway: merchant's ID, transaction amount, merchant's internal order number, and the internal routing number. In step 804 the data is passed securely through the gateway to the isolated internal network.

Step 806 validates the routing number by passing the routing number to the secure server network which converts the routing number to the respective credit card data, number and expiration date. The secure server then passes the credit card data, along with the remaining transaction data to the terminal server, in step 808. The terminal server, preferably a Level III compliant POS terminal, receives the transaction data and converts the merchant ID into the merchant name and the merchant processor merchant ID number. The terminal server then compiles the data and in step 810 transmits the data over the standard credit card authorization network.

The transaction returns to the terminal server. The transaction data is passed back through the secure server where it is re-converted to the surrogate account data and passed

to the intranet server and on to the web server. In step 812 the transaction has been completed. The merchant processor has seen a standard transaction come to them for authorization, and the merchant processor responded in their normal fashion. The merchant has seen a standard credit card transaction being handled in a fully secure manner with only a modest deviation to their standard e-commerce process, and they have completed a purchase for one of their consumers. The consumer has been given full assurance that the transaction conducted over the Internet was handled in such a manner so as to provide complete privacy of the consumer's credit card data. The process then passes back to step 626 in Figure 7.

Figure 9 is a block diagram of the process for establishing a consumer's account with the present invention. In step 900 the consumer initiates the set up of a new account preferably through a website, web server, or by calling a 1-800 phone number.

During the account setup process in step 902, the prospective member provides the following data: full name, primary mailing and shipping address (street addresses only, no post office box numbers), e-mail address, telephone number and fax number if available, last four digits of their social security number, date of birth or some other supplemental security field, general demographic data, and the consumer's chosen four digit designated PIN number.

In step 904 the consumer receives an eight digit inactive surrogate credit card number. In step 906 an internal routing number is assigned, which is never seen by the member.

In step 908 a welcome kit is sent to the consumer with the following data: a member surrogate credit card number, instructions on how to activate the account, instructions on the use of the system, a merchant listing, a member agreement indicating the member accepts the terms and conditions of the agreement upon activation of the account, and general marketing materials, specials, and other relevant data.

In step 910 the consumer calls a toll free number to activate their account. The phone call is answered by a secure PBX VRU (Voice Response Unit) which resides in the

secure area of the network. The VRU is consistent with industry standards by providing an invisible layer of authentication for the user by verifying the phone number that the call is placed from to the phone number contained within the Web server. The VRU prompts the consumer to enter via touch tone telephone number their surrogate credit card number, their pre-selected PIN, and the last four digits of their social security number. When the caller is validated by verifying the entry within the web server, the consumer is prompted to enter their designated credit card data which is verbally repeated back to the caller for further verification. The user is given two opportunities for validation. If denied, the caller is prompted to contact consumer service.

In step 912 the PBX then queries the web server for the routing number assigned to the consumer record. The web server returns the routing number to the PBX which then passes the routing number to the secure server which creates a record for the consumer which contains the routing number and the consumer's designated credit data.

Upon completion and validation, in step 914, the consumer account is "Active" and the consumer may begin making transactions.

Figure 10 is a block diagram of the process for establishing a merchant's membership with the entity providing the service described in the present invention. In step 1002 a merchant requests to be registered with the system.

Step 1004 then attempts to determine if the merchant is qualified to be registered by meeting the following criteria: currently accept Visa and/or MasterCard (either credit or debit), currently has an a-commerce web presence and have has been conducting e-commerce for approximately one year, their defined e-commerce methodology is compatible with the present invention, their e-commerce platform meets the system requirements of the present invention, they meet credit worthiness requirements and are a business in good standing, presumably accomplished through the Dun & Bradstreet directory.

If the merchant is not approved, then the process ends. Upon approval the process passes to step 1006 in which an agreement is executed.

In step 1008 the merchant provides the following data: credit card merchant processor merchant identification number, merchant processor name, appropriate contact data at the merchant processor. The present invention then contacts the merchant processor and obtains the following data: telephone number for routing transaction data, confirms data format utilized for authorizations of card transactions, provides the present invention with a new POS terminal identification assigned to the present inventions Merchant's membership number.

Step 1010 then assigns the merchant a member-merchant identification and creates a record for the merchant within the present invention terminal server. This record includes the following: Merchant ID, merchant name and contact data, processor name and contact data, processor merchant ID, and telephone number for transaction processing.

In step 1012 the present invention then provides the programming required to enable the merchant to accept transactions. This includes working within the merchant's existing platform to offer the present invention as another payment option path to consumers. Embedded within this code is the ability to capture the total transaction purchase price, the merchant's internal order number, the consumer address data and the merchant ID. Upon testing, verification, and certification, the merchant is setup and may begin accepting transactions.

In another embodiment, the surrogate credit card number and/or PIN does not have to be a number, it may be a digital certificate or other means of identifying the consumer.

Obviously, numerous modifications and variations of the present invention are possible in light of the above teachings. It is therefore to be understood that within the scope of the appended claims, the invention may be practiced otherwise than as specifically described herein.

CLAIMS

What is claimed is:

1. A method for facilitating secure electronic commerce without providing a consumers credit card data over a public network in real time, comprising the steps of:

receiving an order request from a merchant;

receiving a consumers' surrogate identification from the consumer;

receiving the consumers' personal identification from the consumer, and

transmitting the consumers' credit card data to the merchants' merchant account processor upon verification that the received surrogate identification matches the received personal identification.

2. A method for facilitating secure electronic commerce as in claim 1, further comprising the step of:

transmitting a purchase authorization screen to the consumer.

3. A method for facilitating secure electronic commerce as in claim 2, further comprising the step of:

determining the internet protocol address of the consumer for the transmission of the purchase authorization screen.

4. A method for facilitating secure electronic commerce as in claim 2, further comprising the step of:

displaying a purchase authorization screen to the consumer for the purpose of obtaining the consumers' surrogate identification and personal identification.

5. A method for facilitating secure electronic commerce as in claim 1, wherein an order request from a merchant comprises: a merchants' ID, a transaction amount, and a merchants' internal order number.

6. A method for facilitating secure electronic commerce as in claim 5 wherein an order request from a merchant further comprises a shipping address.

7. A method for facilitating secure electronic commerce as in claim 5 wherein an order request from a merchant further comprises an internet protocol address of the consumer.

8. A method for facilitating secure electronic commerce as in claim 1, wherein receiving the consumers' surrogate identification and receiving the consumers' personal identification number comprises receiving the surrogate identification and personal identification number directly from the consumer without ever revealing the surrogate identification or the personal identification number to the merchant.

9. A method for facilitating secure electronic commerce as in claim 1, further comprising the step of:

transmitting a notification to the merchant that the transaction has been completed or has not been completed.

10. A method for facilitating secure electronic commerce as in claim 9, further comprising the step of:

receiving a notification from the merchants' merchant account processor that the transaction has been completed or has not been completed.

11. A method for facilitating secure electronic commerce as in claim 9, further comprising the step of:

upon receiving a notification from the merchants' merchant account processor that the transaction has been completed successfully, transmitting the consumers' shipping data to the merchant.

12. A method for facilitating secure electronic commerce as in claim 9, wherein a consumers' surrogate identification is a number.

13. A method for facilitating secure electronic commerce as in claim 9, wherein a consumers' personal identification is a number.

14. A method for facilitating secure electronic commerce as in claim 6, further comprising the step of:

comparing the consumers' shipping address with the shipping address provided by the merchant.

15. A method for facilitating secure electronic commerce as in claim 14, further comprising the steps of:

upon determining the consumers' shipping address is different than the shipping address provided by the merchant:

displaying the shipping address provided by the merchant to the customer, and

requesting another form of identification from the customer to verify the customer would like to have their purchase shipped to the shipping address provided by the merchant.

16. A method for facilitating secure electronic commerce without providing a consumers credit card data over a public network in real time, comprising the steps of:

receiving an order request from a merchant containing an internet protocol address of a consumer, a merchant ID, and a merchant internal order number;

displaying a purchase authorization screen to the customer by transmitting the purchase authorization screen to the internet protocol address sent by the merchant;

receiving a consumers' surrogate identification number and personal identification number from the consumer through the purchase authorization screen;

comparing consumers' surrogate identification number and personal identification number;

upon successful comparison, translation the customers surrogate identification number to the customers actual credit card number;

transmitting the consumers' credit card data to the merchants' merchant account processor, and

upon receiving the merchant account processors' approval, transmitting a confirmation to the merchant that the transaction has been completed successfully.

17. A method for facilitating secure electronic commerce as in claim 1, further comprising the steps of:

receiving the consumers credit card data, and

maintaining the consumers credit card data on a computer which is not connected to a public network.

18. A method for facilitating secure electronic commerce as in claim 17, wherein receiving the consumers credit card data comprises receiving the credit card data through a secure gateway from the consumer over a public exchange system through conventional phone lines to a specific phone number provided by the consumer.

19. A system for facilitating secure electronic commerce without providing a consumers credit card data over a public network in real time, comprising:

a first computer containing consumer credit card data, and

a second computer connected to said first computer containing a point of sale program for processing credit card transactions.

20. A system for facilitating secure electronic commerce as in claim 19, further comprising:

a third computer connected to the internet containing a program for communicating with merchants and communicating with consumers;

a fourth computer securely connected to said third computer for relaying communications from said third computer to said first computer, and

wherein said first computer and said fourth computer are connected.

21. A system for facilitating secure electronic commerce as in claim 19, further comprising:

a public exchange system wherein said first computer contains a program allowing the consumer to enter their credit card data through said public exchange network through a secure gateway into said first computer.

22. A system for facilitating secure electronic commerce as in claim 20, further comprising:

a merchant computer connected to said second computer containing a program for processing credit card transactions.

23. A system for facilitating secure electronic commerce as in claim 19, wherein the point of sale program for processing credit card transactions is a level III compliant terminal.

24. A system for facilitating secure electronic commerce as in claim 20, wherein the security between said fourth computer and said third computer is a firewall.

25. A system for facilitating secure electronic commerce as in claim 19,

wherein said first computer contains a program for converting consumer surrogate credit card data into actual consumer credit card data.

26. A system for facilitating secure electronic commerce as in claim 19,

wherein said first computer contains a program for receiving consumer credit card data over a phone line from a public exchange voice response unit.

27. A system for facilitating secure electronic commerce as in claim 20, wherein the connection between said first computer and said fourth computer is wireless.

28. A system for facilitating secure electronic commerce as in claim 19, wherein the connection between said first computer and said second computer is wireless.

29. A system for facilitating secure electronic commerce as in claim 20, wherein the connection between said third computer and said fourth computer is wireless.

30. A system for facilitating secure electronic commerce as in claim 19, wherein said first computer is not connected to a public network.

31. Computer executable software code stored on a computer readable medium, the code for facilitating secure commerce, electronic commerce without providing a consumers credit card data over a public network in real time, comprising:

code for displaying a pop up window onto a consumers computer containing data regarding a purchase,

code for receiving the consumers identification, and

code for transmitting consumers identification.

Computer executable software code stored on a computer readable medium as in claim 31, further comprising:

code for approving the consumers identification, and

code for completing a credit card transaction upon approval of consumers identification.

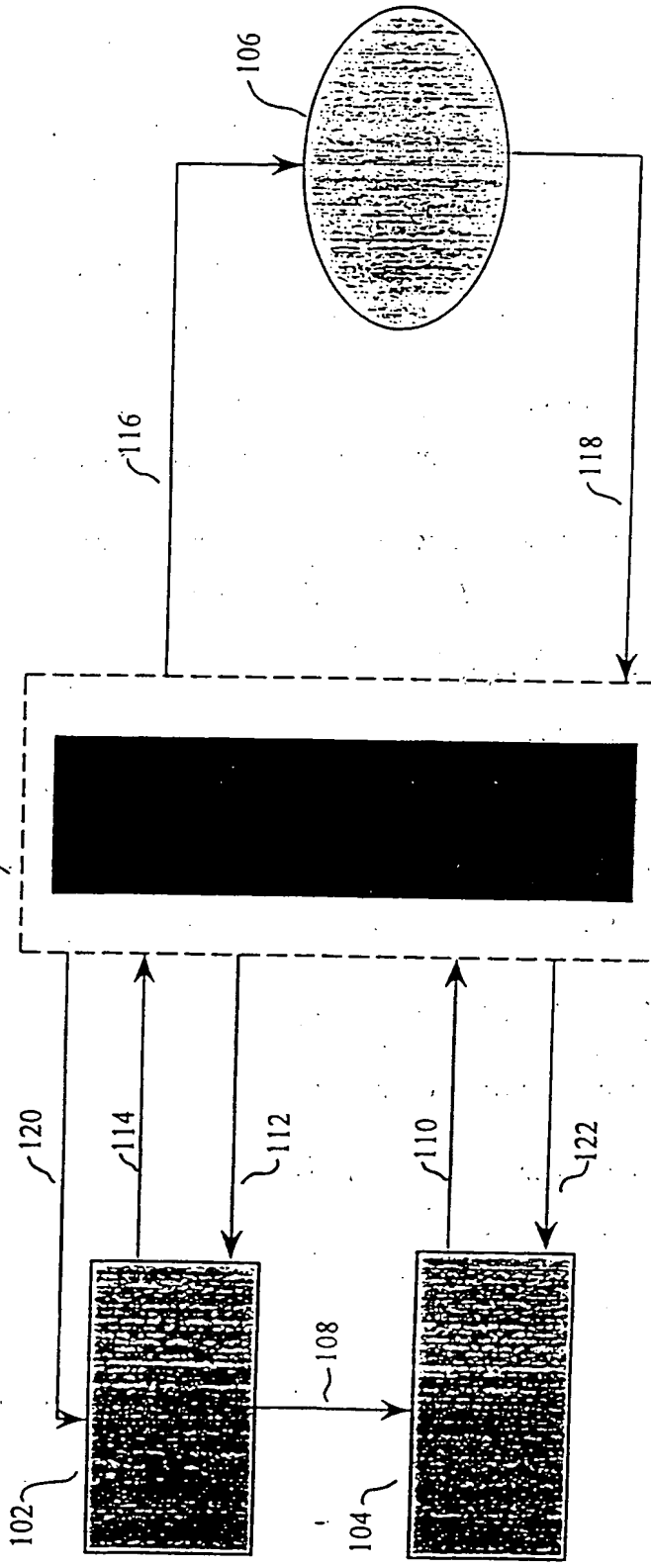


FIGURE 1

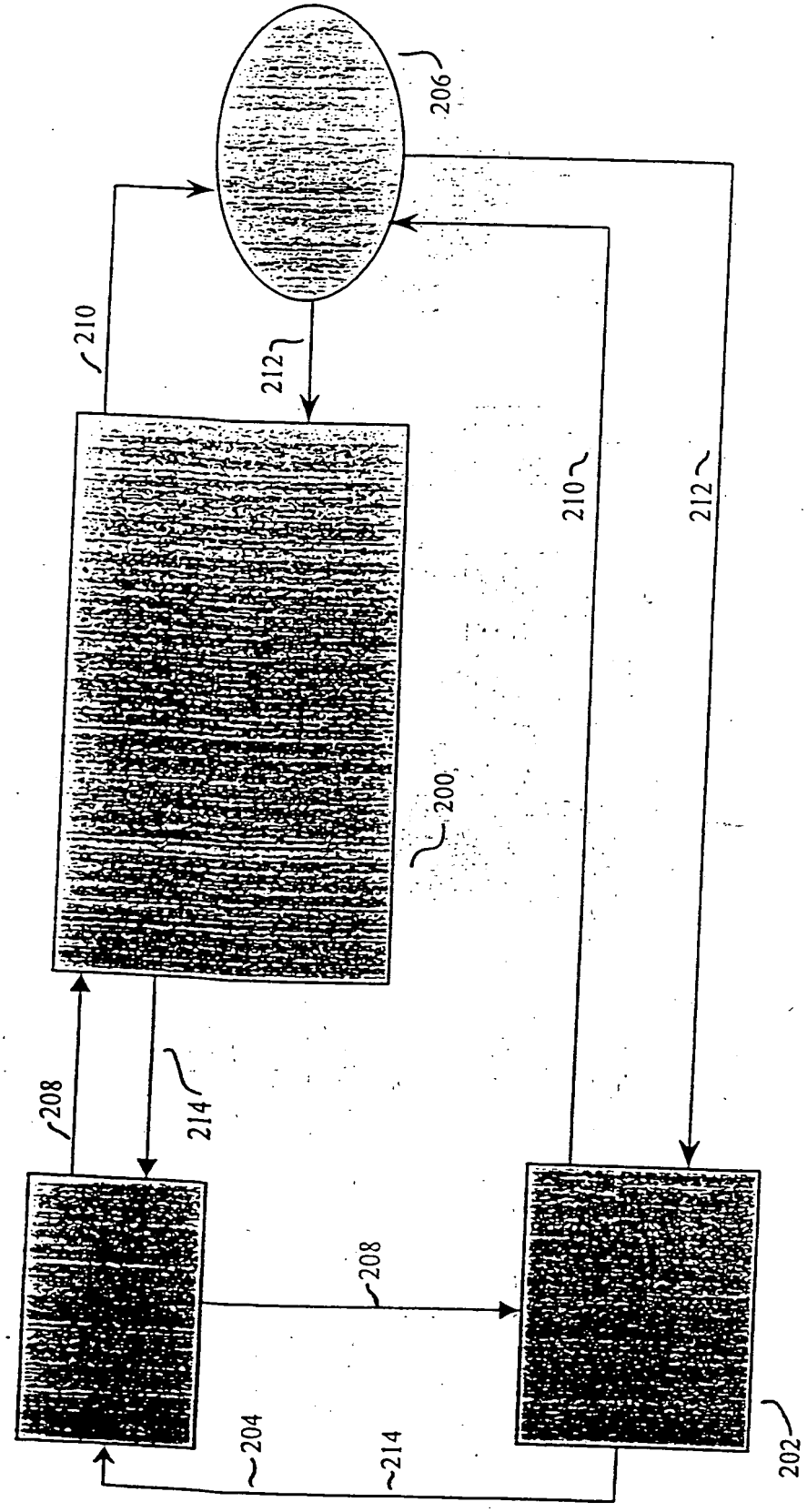


FIGURE 2

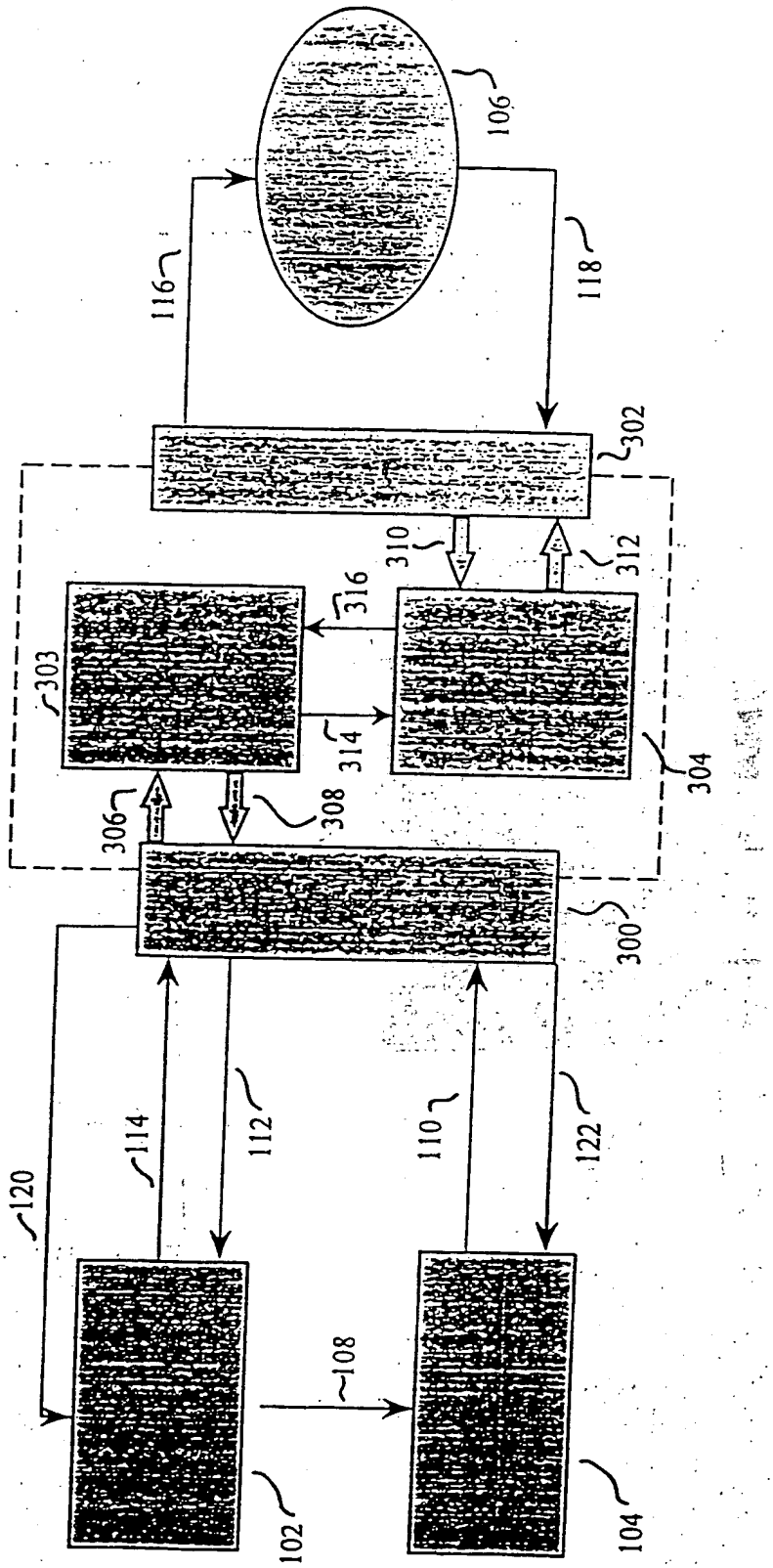

106
116
118
302
310
312
316
303
314
304
306
308
300
120
114
112
110
122
108
102
104

FIGURE 3

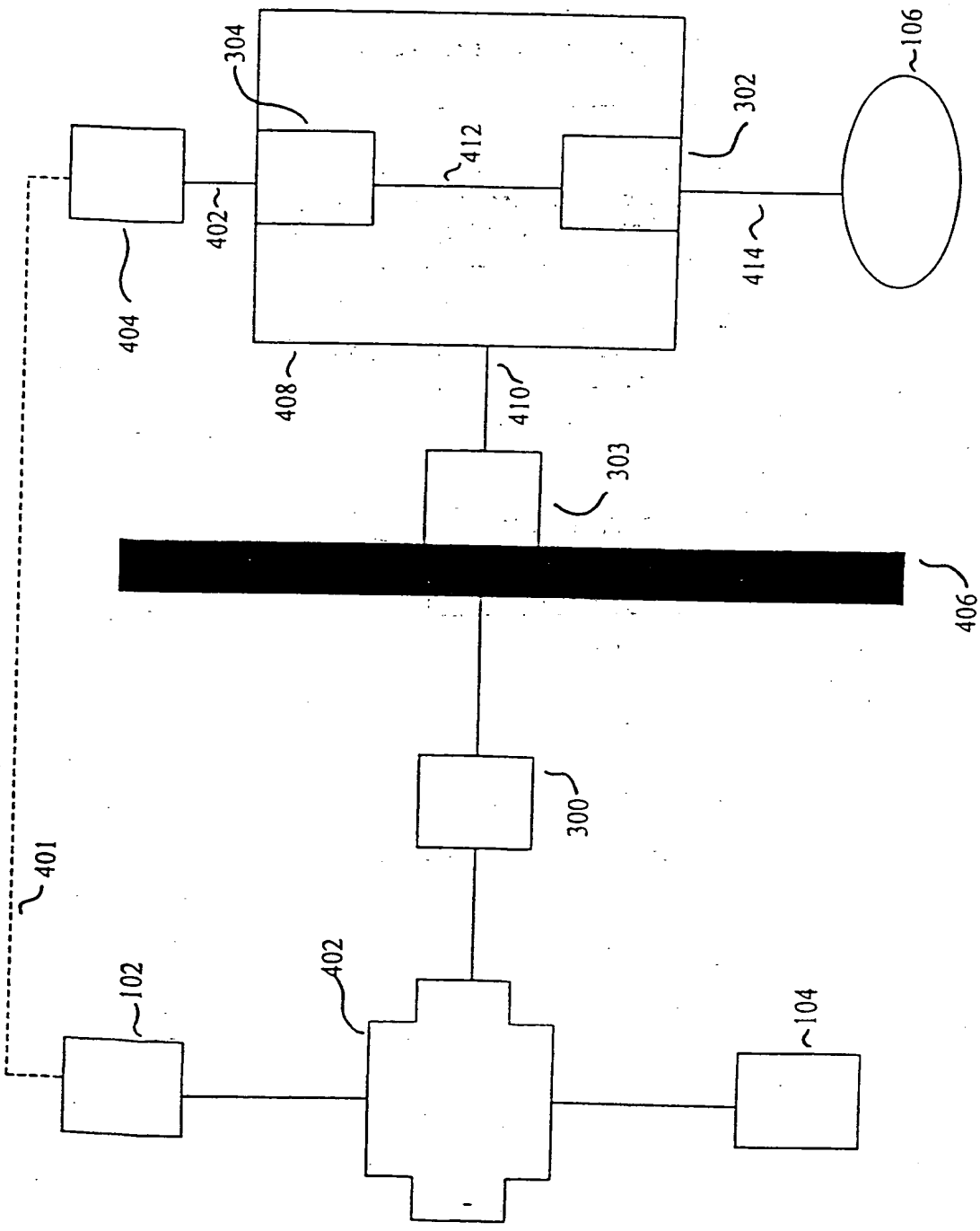


FIGURE 4

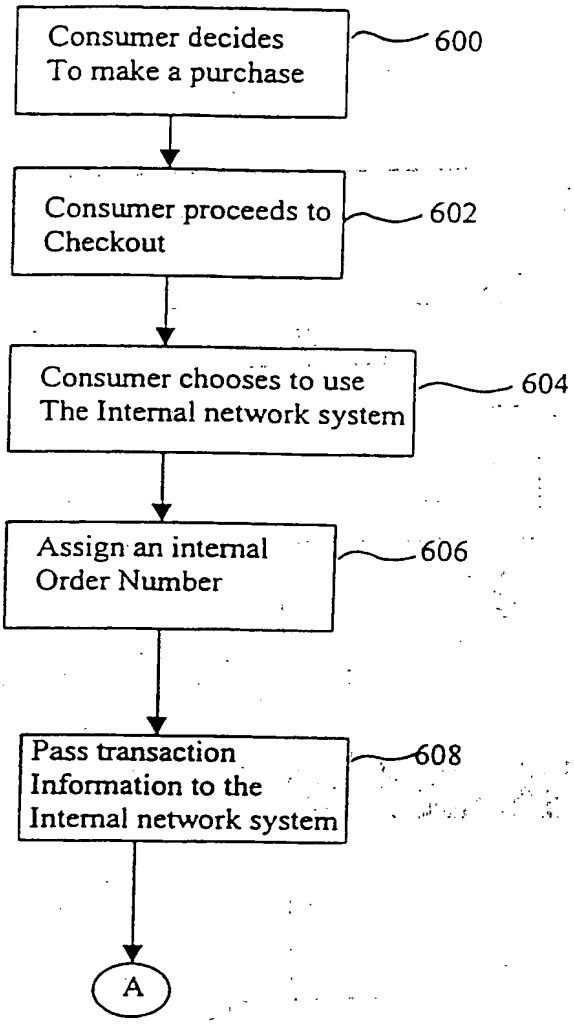

Consumer decides To make a purchase
600
Consumer proceeds to Checkout
602
Consumer chooses to use The Internal network system
604
Assign an internal Order Number
606
Pass transaction Information to the Internal network system
608
A

FIGURE 6

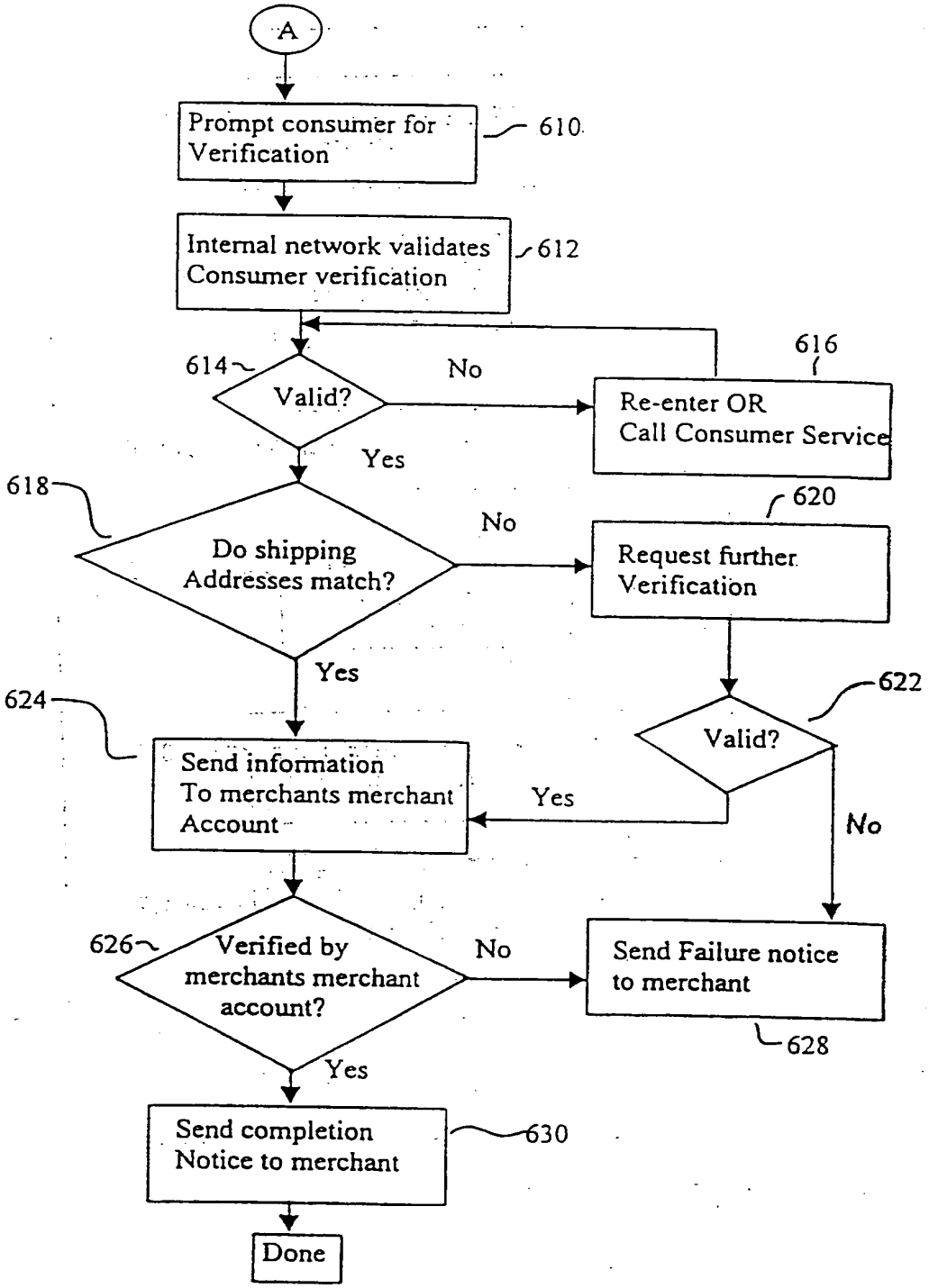


FIGURE 7

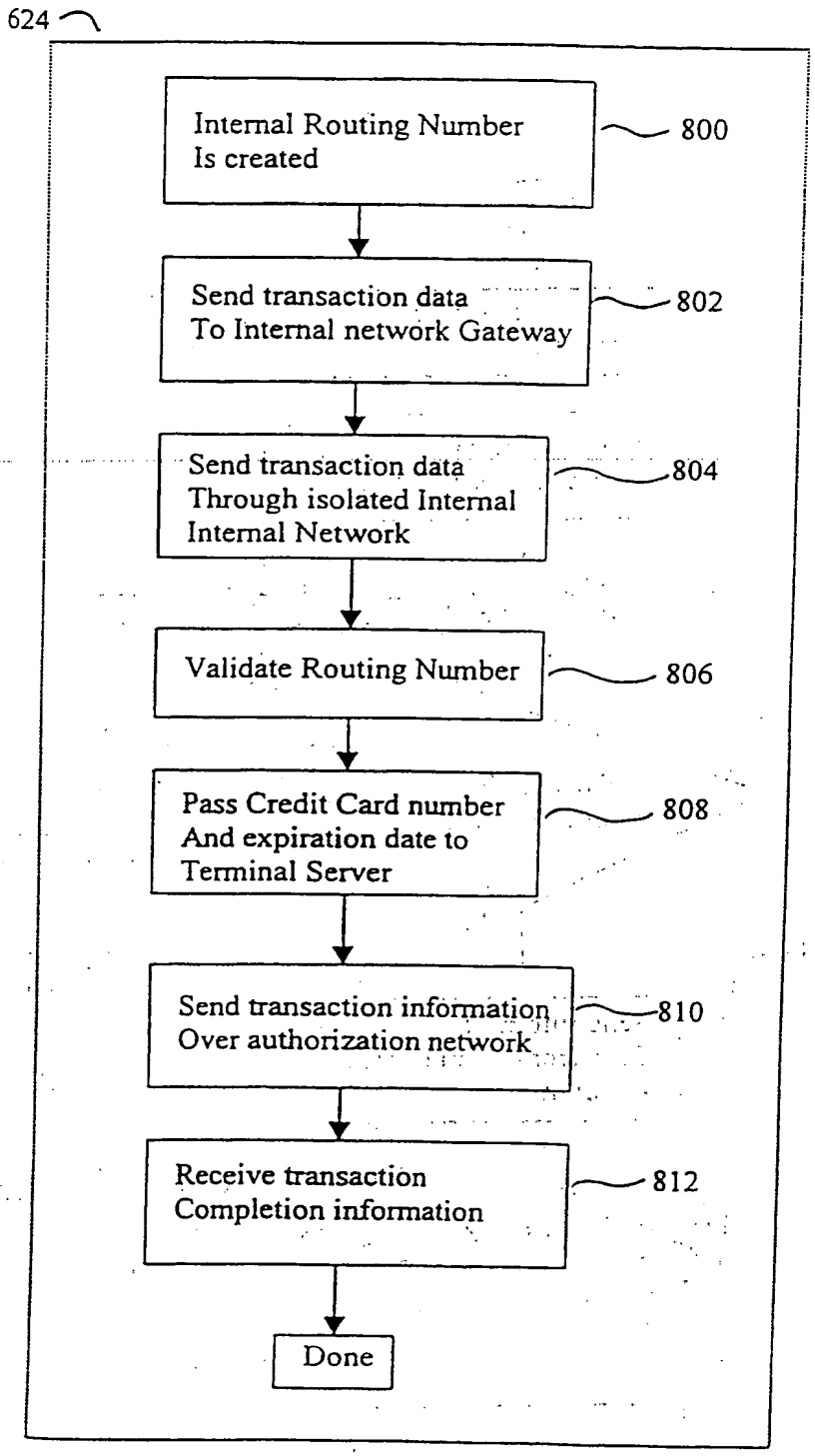


FIGURE 8

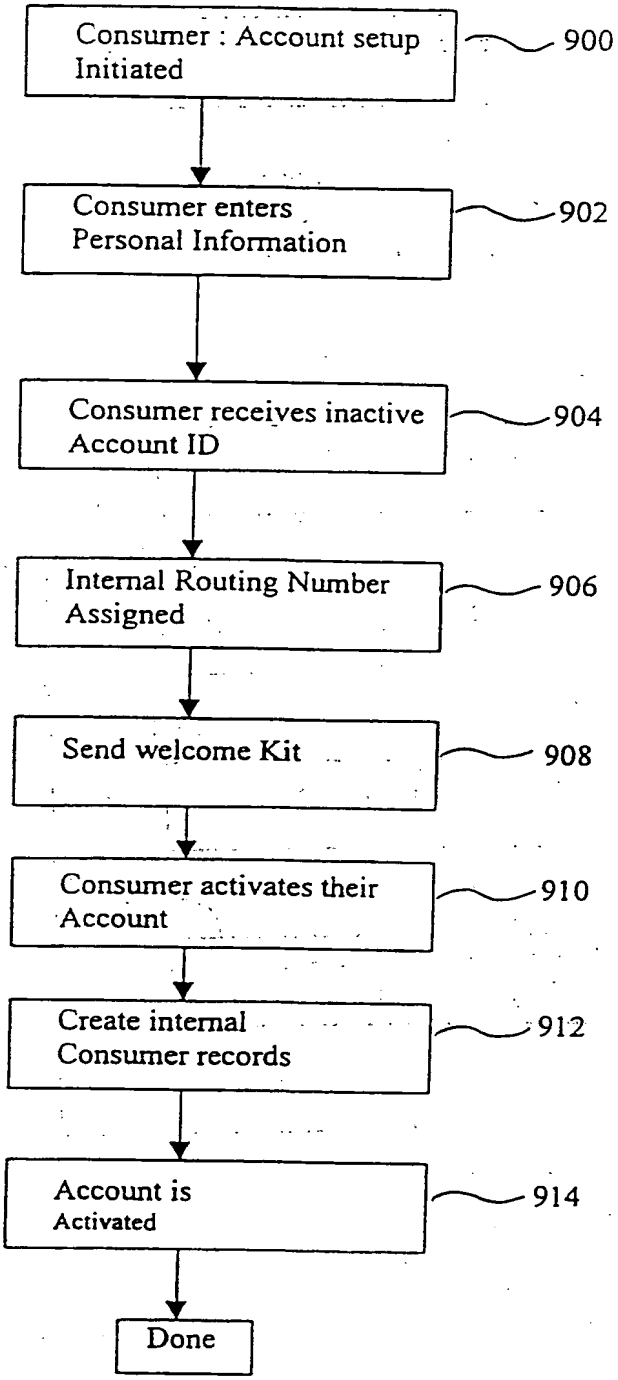


FIGURE 9

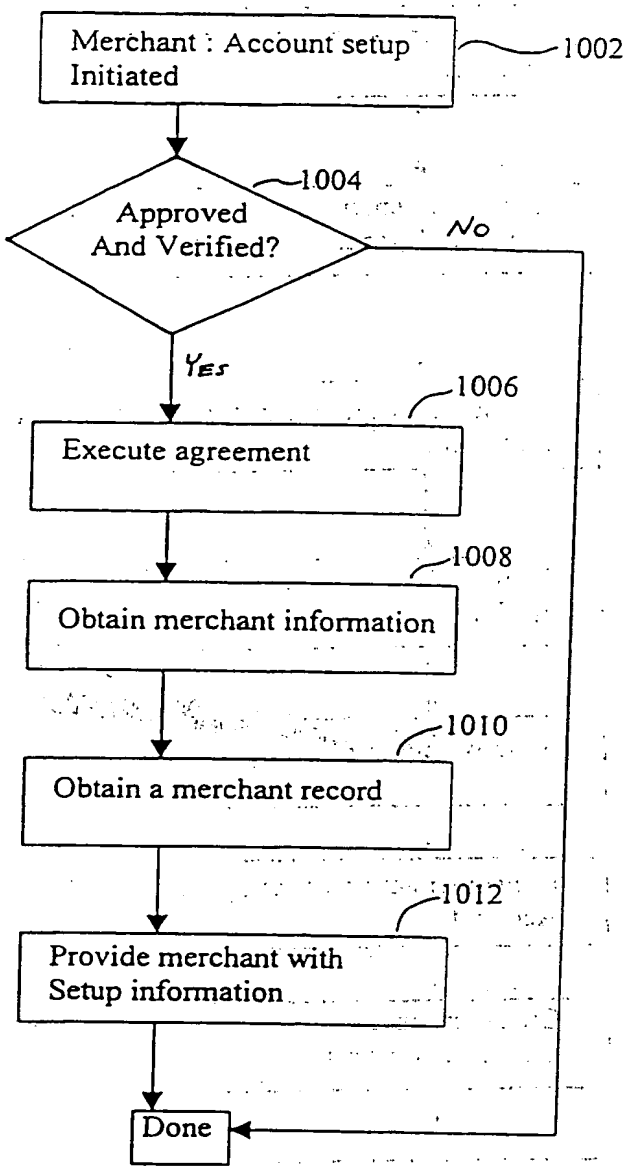


FIGURE 10

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 December 2000 (14.12.2000)

PCT

(10) International Publication Number
WO 00/75749 A3

(51) International Patent Classification[7]: G06F 17/60

(21) International Application Number: PCT/US00/15827

(22) International Filing Date: 8 June 2000 (08.06.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/328,422 9 June 1999 (09.06.1999) US

(71) Applicant *(for all designated States except US)*: INTELISHIELD.COM, INC. [US/US]; 10200 W. 44th Avenue, Suite 339, Wheat Ridge, CO 80033 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: FLOYD, Dennis, R. [US/US]; 3265 Fenton Street, Denver, CO 80212 (US). HEATON, Timothy, L. [US/US]; 10875 W. 77th Drive, Arvada, CO 80005 (US). ANDERSON, Brian, S. [US/US]; 8755 W. 80th Avenue, Arvada, CO 80005 (US). ANDERSON, Stanley, W. [US/US]; 8755 W. 80th Avenue, Arvada, CO 80005 (US).

(74) Agent: FOLEY & LARDNER; 777 East Wisconsin Avenue, 33rd Floor, Milwaukee, WI 53202-5367 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

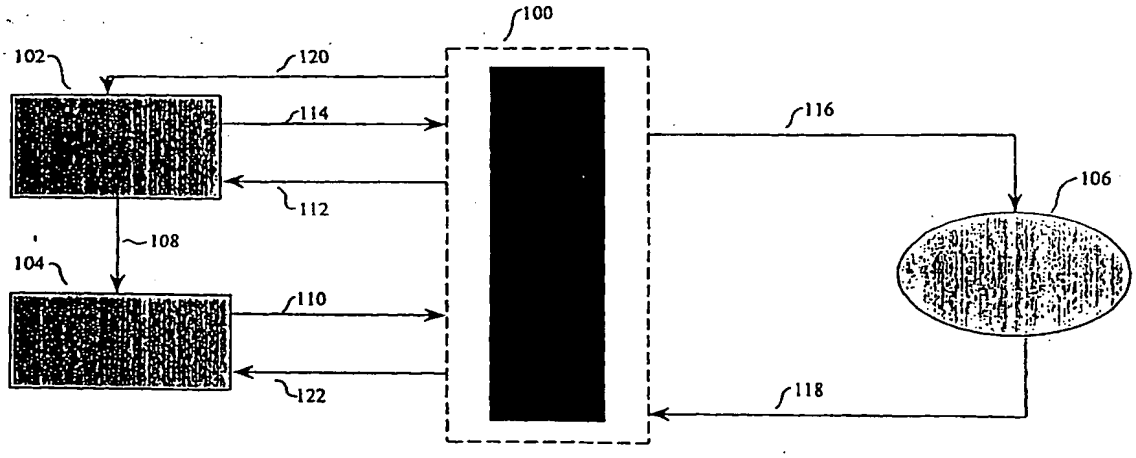
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*
— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

(88) Date of publication of the international search report:
1 February 2001

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: INTERNET PAYMENT SYSTEM



(57) Abstract: The present invention is a system and method for providing electronic commerce without providing a consumer's (102) credit card data over the Internet, or any other public network. Consumers (102) have a fear of providing their credit card data over the Internet. The present invention allows a consumer to make a purchase with their credit card without providing their credit card data over the Internet. The present invention provides consumers (102) with a surrogate card number to make Internet purchases and the consumer (102) personally authorizes their purchases while they are on-line. The consumer's actual credit card data is never transmitted over the Internet. The on-line affirmation of each purchase through the third party entity that provides the service described by this invention leads to a reduction of fraud.

WO 00/75749 A3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/15827

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) :G06F 17/60
US CL :705/26
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 705/26,16,18,1,500;341/173,174,899,50,51,52

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EAST, WEST, STN

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,P	US 6,023,682 A (CHECCHIO) 08 February, 2000, col. 1, line 66-col. 2, line 25, col. 3, lines 1-11, col. 4, lines 13-31	19,26
Y,P		1, 12, 13, 20-25, 27-30, 31, 32
Y	US 5,903,721 A (SIXTUS) 11 May 1999, col. 1, lines 5-10, col. 3, line 37-col. 4, line 14, col. 6, lines 36-45, col. 7, lines 37-47,	1-16, 31, 32

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 23 AUGUST 2000	Date of mailing of the international search report 27 NOV 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer TOD SWANN Telephone No. (703) 308-7791

Form PCT/ISA/210 (second sheet) (July 1998)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/15827

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,727,163 A (BEZOS) 10 March 1998, col. 1, line 62-col. 2, line 8, col. 7, lines 57-63, col. 8, lines 10-22	1-18, 31, 32
Y	US 5,890,137 A (KOREEDA) 30 March 1999, col. 9, lines 5-61, col. 10, lines 63-67	2-4, 16
Y	US 5,825,881 A (COLVIN, SR.) 20 October 1998, col. 2, lines 7-14, col. 3, lines 21-23, col. 5, lines 40-41, col 7, lines 17-26, col. 10, line 64-col. 11, line 9, col. 24, line 48-col. 25, line 8	5-11, 14, 15
Y	US 5,903,652 A (MITAL) 11 May 1999, Figure 1, abstract, lines 15-25	20-25, 27-30
Y	US 5,757,917 A (ROSE et al) 26 May 1998, col. 4, lines 53-65	24